Fraunhofer SIT

1. Summary

Vendor: Twitter Inc.

Product: TwitterKit for iOS

Affected Version: <= 3.4.2

CVSS Score: 8.1 (High)
(https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N)

Severity: high

Remote exploitable: yes

The Twitter Kit framework through 3.4.2 for iOS does not properly validate the api.twitter.com SSL certificate. Although the certificate chain must contain one of a set of pinned certificates, there are certain implementation errors such as a lack of hostname verification. NOTE: this is an end-of-life product.

Description

The vulnerability was acknowledged by Twitter via HackerOne on July 9th, 2019 (Report #560584). However, no fix will be supplied, as TwitterKit is end of life affective October 31, 2018. This leaves thousands of apps vulnerable. A quick scan of the German top 2000 apps revealed at least 45 affected apps (May 2019).

The Twitter Kit for iOS framework uses a vulnerable certificate validation implementation. The certificate validation only verifies that the received certificate chain contains one of the 21 pinned root certificates. The domain name it NOT verified. So any valid certificate that was issued by one of the 21 pinned CAs is accepted by the implemented trust evaluator. An attacker with a valid certificate for his own domain, issued by one of these CAs, can use this certificate for man-in-the-middle-attacks against app communicating via the Twitter Kit for iOS with api.twitter.com.

The TWTRServerTrustEvaluator class contains the following SHA-1 Hashes of the pinned public keys:

```
"1a21b4952b6293ce18b365ec9c0e934cb381e6d4",  // "VERISIGN_CLASS3_G2"
"2343d148a255899b947d461a797ec04cfed170b7",  // "VERISIGN_CLASS1"
"5519b278acb281d7eda7abc18399c3bb690424b5",  // "VERISIGN_CLASS1_G3"
"1237ba4517eead2926fdc1cdfebeedf2ded9145c",  // "VERISIGN_CLASS2_G2"
"5abec575dcaef3b08e271943fc7f250c3df661e3",  // "VERISIGN_CLASS2_G3"
"22f19e2ec6eaccfc5d2346f4c2e8f6c554dd5e07",  // "VERISIGN_CLASS3_G3"
"ed663135d31bd4eca614c429e319069f94c12650",  // "VERISIGN_CLASS3_G4"
"b181081a19a4c0941ffae89528c124c99b34acc7",  // "VERISIGN_CLASS3_G5"
"3c03436868951cf3692ab8b426daba8fe922e5bd",  // "VERISIGN_CLASS4_G3"
"bbc23e290bb328771dad3ea24dbdf423bd06b03d",  // "VERISIGN_UNIVERSAL"
"c07a98688d89fbab05640c117daa7d65b8cacc4e",  // "GEOTRUST_GLOBAL"
"713836f2023153472b6eba6546a9101558200509",  // "GEOTRUST_GLOBAL2"
"b01989e7effb4aafcb148f58463976224150e1ba",  // "GEOTRUST_PRIMARY"
"bdbea71bab7157f9e475d954d2b727801a822682",  // "GEOTRUST_PRIMARY_G2"
"9ca98d00af740ddd8180d21345a58b8f2e9438d6",  // "GEOTRUST_PRIMARY_G3"
"87e85b6353c623a3128cb0ffbbf551fe59800e22",  // "GEOTRUST_UNIVERAL"
"5e4f538685dd4f9eca5fdc0d456f7d51b1dc9b7b",  // "GEOTRUST_UNIVERSAL2"
"d52e13c1abe349dae8b49594ef7c3843606466bd",  // "DIGICERT_GLOBAL_ROOT"
"83317e62854253d6d7783190ec919056e991b9e3",  // "DIGICERT_EV_ROOT"
"68330e61358521592983a3c8d2d2e1406e7ab3c1",  // "DIGICERT_ASSUREDID_ROOT"
"56fef3c2147d4ed38837fdbd3052387201e5778d",  // "TWITTER1"
```

see https://github.com/twitter/twitter-kit-ios/blob/master/TwitterCore/TwitterCore/Networking/Security/TWTRServerTrustEvaluator.m

In method `evaluateServerTrust:(SecTrustRef)serverTrust forDomain:(NSString *)domain` each certificate of the received certificate chain is checked against the above list. If one fits, the connection is accepted. So for example any valid certificate chain signed with a VeriSign_Class1 root certificate is accepted, as no further checks are performed that verify the domain name.

This certificate validator is called by `TWTRURLSessionDelegate`.
see: https://github.com/twitter/twitter-kit-ios/blob/v3.2.1/TwitterCore/TwitterCore/Networking/Pipeline/TWTRURLSessionDelegate.m

However, this delegate does not invoke `secTrustEvaluate`, which would evaluate trust for the specified certificate and policies. Additionally, the host name is not verified.
see https://developer.apple.com/documentation/security/1394363-sectrustevaluate?language=objc

Steps To Reproduce

The vulnerability was practically verified with apps using TwitterKit for iOS.

An http-proxy was used to redirect requests for `api.twitter.com` to a server with a certificate signed by one of the pinned CAs. This was done by assigning `api.twitter.com` an IP of a server under our control. As long as the certificate of this server was signed by a pinned CA, the connection was established successfully, although we should not be able to establish a secured connecting for domain `api.twitter.com`. On this server, we receive the transmitted http data and proxy it to a connection established to the real Twitter server.

Impact

We are aware that Twitter has discontinued support for Twitter Kit. However, we have still detected vulnerable versions of this framework in many apps, as the framework is also included in other 3rd party frameworks like Google Fabric.

Users of these apps are exposed to the risk of identity theft, account abusage and loss of privacy.

A quick scan of the German top 2000 apps revealed at least 45 affected apps (May 2019).

2. Workaround

In affected apps, the feature to use Twitter should not be used.

3. Possible fix

Twitter has acknowledged the vulnerability, but no fix for TwitterKit for iOS will be released by Twitter, as TwitterKit reached end of life October 31, 2018.

Developers need to switch to alternative APIs, see:
https://blog.twitter.com/developer/en_us/topics/tools/2018/discontinuing-support-for-twitter-kit-sdk.html