Security Advisory SWRX-2016-001

Facebook Messenger (iOS) Certificate Validation Vulnerability

Dell SecureWorks Counter Threat Unit™ Threat Intelligence

Advisory Information

Title: Facebook Messenger (iOS) Certificate Validation Vulnerability
Advisory ID: SWRX-2016-001
Advisory URL: https://www.secureworks.com/research/swrx-2016-001
Date published: Tuesday, March 22, 2016
CVE: Not assigned
CVSS v2 base score: 5.8
Date of last update: Tuesday, March 22, 2016
Vendors contacted: Facebook, Inc.
Release mode: Coordinated
Discovered by: Sean Wright, Dell SecureWorks

Summary

The Facebook social networking service includes a mobile application called Messenger that allows users to send private messages to their Facebook contacts. Although the application uses HTTPS to communicate with the backend servers, insufficient validation of the certificates returned by these servers leaves the application open to man-in-the-middle (MITM) attacks.

Affected products

This issue affects Messenger iOS version 57.0 if the iOS device is configured to use a proxy. Android versions of the application are unaffected by this vulnerability.

Vendor information, solutions, and workarounds

Affected users should upgrade Messenger iOS to version 59.0 or later. An alternative is to use a direct connection and not configure iOS to use a proxy.

Details

Version 57.0 of Facebook's mobile Messenger application does not perform appropriate certificate validation if the iOS device is configured to use a proxy:

- The Certificate Authority that signs the server certificate is not validated.
- The Common Name (or Subject Alternative Name) field on the certificate is not validated.

This lack of validation could allow an attacker to generate a certificate and conduct an MITM attack. The threat actor could obtain the application's OAuth Authorization token, as well as other potentially sensitive information, and could manipulate the response from the server to the application to conduct additional attacks against a victim.

CVSS severity (version 2.0)

Access vector: Network
Access complexity: Medium
Authentication: None
Impact type: Information disclosure, allows unauthorized modification
Confidentiality impact: Partial
Integrity impact: Partial
Availability impact: None
CVSS v2 base score: 5.8
CVSS v2 impact subscore: 4.9
CVSS v2 exploitability subscore: 8.6
CVSS v2 vector: (AV:N/AC:M/Au:N/C:P/I:P/A:N/E:POC/RL:U/RC:C)

Proof of concept

The vulnerability was discovered when using a local proxy:

- The local proxy reissued and signed the server certificate with its own certificate, which was not in the iOS Trust Store (Profiles). This behavior indicates that the Messenger application does not validate the certificate authority that signed the server certificate presented to the application.
- A setting on the local proxy caused it to present a certificate with the Common Name "invalid-host.com". Messenger still honored the certificate, indicating that it did not validate the Common Name (or Subject Alternative Name) field of the presented certificate.

The following steps can reproduce the issue with a local proxy:

1. Download Burp Suite from PortSwigger (Java must be installed).
2. Configure Burp Suite as the proxy.
   a. Open Burp Suite and select the Proxy tab.
   b. Click the Options sub-tab.
   c. In the Proxy Listeners section, click the Edit button.
   d. In Bind to address, select "All interfaces."
   e. Click Ok.
   f. Click the Http History sub-tab and monitor the logs for traffic going to the Facebook servers.
3. Configure an iPhone/iPad to point to the Burp Suite proxy.
   a. Join the same network as the Burp Suite proxy.
   b. Click the Settings icon and select Wi-Fi.
   c. Press the i (information) icon to the right of the current Wi-Fi connection.
   d. Scroll to the HTTP Proxy section at the bottom of the screen and select "Manual."
   e. Enter the IP address of the server/PC running Burp Suite (referred to as the burp_suite_proxy_ip in step 4).
   f. Enter "8080" in the Port field.
4. Open a web browser on the iPhone/iPad and navigate to http://<*burp_suite_proxy_ip*>:8080 to access the Burp Suite landing page.
5. In the same browser, navigate to https://www.google.co.uk. The browser should present a certificate error.

6. Open the Facebook Messenger mobile application and ensure that it loads correctly.
7. View the Http History in Burp Suite and confirm that the traffic was sent to the Facebook mobile servers (graph.facebook.com, api.facebook.com, cdn.fbsbx.com, external.xx.fbcdn.net).

Revision history

1.0 2016-03-22: Initial advisory release

PGP keys

This advisory has been signed with the Dell SecureWorks Counter Threat Unit™ PGP key, which is available for download at https://www.secureworks.com/~/media/Files/Keys/SecureWorksCTU1.ashx?la=en.

About Dell SecureWorks

Dell Inc. listens to clients and delivers worldwide innovative technology and business solutions they trust and value. Recognized as an industry leader by top analysts, Dell SecureWorks provides world-class information and IT security services to help organizations of all sizes protect their IT assets, comply with regulations and reduce security costs.

Disclaimer