Trustwave®
Information Security & Compliance

April 29, 2014

Thami Smires
Chief Technology Officer
CHARGE Anywhere LLC

CHARGE Anywhere LLC engaged Trustwave, operating under TrustWave Holdings, Inc. ("Trustwave") to conduct a third party security assessment and determine whether CHARGE Anywhere LLC has satisfactorily met the Payment Card Industry (PCI) Payment Application Data Security Standard (PA-DSS) version 2.0 requirements related to the protection of cardholder data. Trustwave is an authorized third party assessor for all the major payment card associations. Currently, the PCI-SSC does not consider payment applications running on mobile platforms to be in scope for PA-DSS certification. As such, Trustwave used the data security standards set forth in the PA-DSS requirements to determine the applications' overall security posture when implemented in a PCI-DSS "in-scope" environment and assessed the application against every requirement in the PA-DSS standard. These include but are not limited to:

- Storage of sensitive authentication data after authorization (PADSS 1.1.x)
- Mask PAN when displayed (PADSS 2.2)
- Render Payment Application passwords unreadable (PADSS 3.3)
- Implementation of SSL/TLS (PADSS 11.1)
- Never send unencrypted PANs via email (PADSS 11.2)
- Implementation Guide for Merchants

The following business units and platforms were in scope for this assessment:

Charge Anywhere (MPOS) Mobile Payment Application 2.1.0 on Apple iOS

Trustwave has completed laboratory testing of the application and a complete review of all PA-DSS requirements. No negative issues were discovered.

Sincerely,

Keith Swiat
Director, Payment Application Practice, Trustwave

70 W. Madison St.
Suite 1050
Chicago, IL 60602

tel 312 873 7500
fax 312 443 8028
www.trustwave.com

Trustwave®
Information Security & Compliance

Mobile Application Review Report

Name of Application: Charge Anywhere (MPOS) Mobile Payment Application

Version: 2.1.0

Platforms tested:

- Apple iOS 6.1.3

Devices used for testing:

- Apple iPad Mini
- Woosim Systems WSP-R240 Bluetooth Mobile Printer and Magnetic Stripe Reader
- Miura Shuttle Bluetooth Mobile Magnetic Stripe Reader, EMV Reader, and Debit PIN Pad
- IDTECH Audio Jack Magnetic Stripe Reader

Types of Transactions supported:

- Card Present (Track data collected)
- Manually Entered with CVV2
- PIN based Debit
- EMV Credit and Debit

Cardholder data storage:

- Track, CVV2 and PIN block (for EMV debit transactions) may be stored prior to authorization in offline mode. All data is stored encrypted with 256-bit AES in the database (Chargeanywhere.sqlite) and securely deleted after successful authorization (when system is back online) or when the logs are rotated. Track, CVV2 and PIN block data are not stored post authorization.
- PAN stored Encrypted using 256-bit AES when needed.
- No leaked clear text cardholder data was found during analysis of forensic data collected.

Relevant Compliance Observations:

- Offline mode is supported.
- Full PANs are not printed on merchant receipts.
- All users have unique ID's and password security, in accordance with PA-DSS password requirements (PA-DSS 3.1), is enforced.

70 W. Madison St.
Suite 1050
Chicago, IL 60602

tel 312 873 7500
fax 312 443 8028
www.trustwave.com

Trustwave®
Information Security & Compliance

Implementation of SSL/TLS (PADSS 11.1)

Test transactions were processed and network traffic captured during testing. An analysis of that data shows the following data.

All test transactions were sent to a test payment gateway at 65.211.79.40 on port 443.

Android

Supported Client-side Protocol: TLS 1.0 (0x0301)

Supported Cipher suites:

TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
TLS_ECDHE_ECDSA_WITH_RC4_128_SHA (0xc007)
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc008)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026)
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025)
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a)
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029)
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)
TLS_ECDH_ECDSA_WITH_RC4_128_SHA (0xc002)
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc003)
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
TLS_ECDH_RSA_WITH_RC4_128_SHA (0xc00c)
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA (0xc00d)
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
TLS_RSA_WITH_RC4_128_SHA (0x0005)
TLS_RSA_WITH_RC4_128_MD5 (0x0004)
TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067)
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006b)
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x0016)
TLS_ECDHE_ECDSA_WITH_NULL_SHA (0xc006)
TLS_ECDHE_RSA_WITH_NULL_SHA (0xc010)
TLS_ECDH_ECDSA_WITH_NULL_SHA (0xc001)
TLS_ECDH_RSA_WITH_NULL_SHA (0xc00b)
TLS_RSA_WITH_NULL_SHA256 (0x003b)
TLS_RSA_WITH_NULL_SHA (0x0002)
TLS_RSA_WITH_NULL_MD5 (0x0001)

Elliptical Curve Extension Supported: YES

Connected Protocol and Cipher suite:

Connected Protocol: TLS 1.2 (0x0303)
Connected Cipher suite: TLS_RSA_WITH_RC4_128_SHA

Analysis: Weak supported client side cipher suites were found. The following cipher suites are considered weak since they do not encrypt connections:

TLS_ECDHE_ECDSA_WITH_NULL_SHA (0xc006)
TLS_ECDHE_RSA_WITH_NULL_SHA (0xc010)
TLS_ECDH_ECDSA_WITH_NULL_SHA (0xc001)
TLS_ECDH_RSA_WITH_NULL_SHA (0xc00b)
TLS_RSA_WITH_NULL_SHA256 (0x003b)
TLS_RSA_WITH_NULL_SHA (0x0002)
TLS_RSA_WITH_NULL_MD5 (0x0001)

Remediation: Currently, these cipher suites are under Apple control and cannot be modified in development. This may change in the future, so continue to monitor Apple development bulletins and change the supported cipher suites (to remove the weak cipher suites) if and when Apple allows this change.

70 W. Madison St.
Suite 1050
Chicago, IL 60602

tel 312 873 7500
fax 312 443 8028
www.trustwave.com