MatrixSSL 3.2.1 Open Source Release Notes

PeerSec Networks, Inc. 410 Broadway Ave E. #205 Seattle, WA 98102 **T** 425.646.7850 **F** 206.501.4366

support@peersec.com www.peersec.com

Overview

Thank you for choosing MatrixSSL. The 3.2 version is a minor revision to the 3.1 releases and adds TLS 1.1 protocol support in addition to a handful of other changes. The latest 3.1 version is MatrixSSL 3.1.4

If you are migrating from a 2.x version of MatrixSSL please contact PeerSec Networks for documentation that can help with the upgrade process.

Who Is This Document For?

- Software developers that are securing applications with MatrixSSL
- Software developers upgrading to MatrixSSL 3.2.1 from a previous version
- Anyone wanting to learn more about MatrixSSL

MatrixSSL 3.2.1 Release Notes

This section highlights the differences between version 3.2.0 and 3.2.1

Feature Addition

PKCS#8 Parsing Added for Parsing Memory Buffer Keys

MatrixSSL 3.2.0 included default PKCS#8 parsing when reading PEM keys from files. This version adds default support for PKCS#8 parsing formats when reading binary keys from memory locations.

Bug Fix

Multiple App Data Records Parsing in TLS 1.1

MatrixSSL 3.2.0 did not correctly parse multiple application data records if they were in a single flight of traffic. **This is an important bug fix if using MatrixSSL 3.2.0 and TLS 1.1**.

Minor Tweaks

Client will not create CLIENT_HELLO if no valid cipher suites are found

If the user has not loaded the correct key material to match the set of enabled cipher suites the CLIENT_HELLO message will not be created and an error will be returned from `matrixSslNewClientSession`.

Disabled REHANDSHAKE_TEST in Client Application

The default *client.c* compile performed a re-handshake test after the initial server connection. This could cause a bit of confusion if the user was using the default client to test a connection to a server that does not support re-handshaking.

Removed the use of likely( ) and unlikey( )

These GCC branch hint macros have been removed from the code due to underuse and namespace collision.

Support and Bug Reporting

Contacting Support or Reporting Bugs

Email support@peersec.com