MatrixSSL 1.8.8 Security Notes

A security flaw in the TLS/SSL protocol related to re-handshaking has been identified and demonstrated. This 1.8.8 release disables servers from re-handshaking. This is a temporary solution that will be updated in future releases when an IETF sponsored fix is formalized.

Summary:
A new attack vector on the TLS/SSL protocol that uses TLS renegotiation has been identified and demonstrated in HTTPS environments. The impact is that a man-in-the-middle can inject plain-text traffic into an authenticated client-server exchange such that the HTTP server will accept and process the request as if it came from the client. This enables the attacker to execute operations on the server using the client's authenticated credentials. The attacker does not see responses. The client may be unaware of the attack.

Threat:
The attack is complex and requires a man-in-the-middle to intercept and relay traffic between the client and server. The attacker establishes an SSL connection with the server, sends partial application data (HTTP) and then initiates a SSL handshake with the authentic client. From the server perspective, this looks like a re-handshake and the partial data sent from the attacker is now associated with the authentic client. The attacker effectively removes himself from the newly negotiated connection so can not receive the server response.

Discussion
Marsh Ray, a software developer with PhoneFactor identified the issue in October this year. See the Renegotiating_TLS PDF file in this directory for more information.

Remedy:
Because this is a TLS/SSL protocol flaw, mitigation options are limited. Eventually (hopefully soon) there will be an IETF sponsored protocol level fix. This may break compatibility with existing clients. A possible, temporary work-around is to disable all renegotiation which does prevent the attack.

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