6
June
2011

This Issue

digicert®
Your Success is Built on Trust™

TLS Renego Man-in-the-Middle Attack

Patches available to fix this security flaw

During the TLS/SSL handshake process, a client and a server communicate encryption parameters to establish a secure connection. However, this process allows both clients and servers to initiate a renegotiation of the encryption parameters.

This renegotiation ability contained a gap in the handshake process where an attacker could intercept the communications between the client and the server in what is known as a TLS Renego Man-in-the-Middle attack.

Since this discovery, most system manufacturers have released patches to fix this flaw but nearly half of the systems using TLS/SSL on the Internet have not installed these necessary patches.

Members of the CA/Browser forum are making a concerted effort to inform organizations of this potential issue. We would like to make it clear that this is not a weakness in DigiCert SSL certificates, but rather a vulnerability in the way systems and browsers initiate the SSL handshake.

You can test your system and ensure that secure renegotiation is enabled by visiting the DigiCert certificate help page. Enter your domain and look for "Secure Renegotiation" under the "SSL certificate" heading. For more information or help with enabling secure renegotiation, visit our TLS Renegotiation page.

Night at the Movies

DigiCert is hosting our Night at the Movies event again for the epic conclusion of the Harry Potter movies. Our Harry Potter and the Deathly Hallows Part 2 movie night will be held on Thursday, July 14th, one day before the film's public release date.

We are excited to bring our event to Boston, MA and Salt Lake City, UT and we look forward to watching the final Harry Potter movie with all of our guests!

DigiCert Managed PKI

Enterprise system for high-volume customers

DigiCert's Managed Public Key Infrastructure (PKI) system empowers customers who require a high SSL certificate volume to take control of certificate management and perform key life-cycle events on demand. It is a forward-thinking interface that keeps the system administrator in mind.

Some of the key features of Managed PKI include:

- Administrative certificate control
- Organization of certificates within Business Units
- Non-expiring account funds
- And much more...

Enterprise managedpki

For questions about the DigiCert Managed PKI system or enterprise accounts, please call our sales team toll free at 1-855-800-3444 or send an email to enterprise@digicert.com.

Follow DigiCert on Twitter and Facebook

Get involved through social media

Following DigiCert on Twitter and/or Facebook is a great way to get involved with a community of peers to discuss topics such as SSL, authentication, and encryption. You can also learn more about what's going on in the Internet security industry through the articles and breaking news items that we post as well.

Updates on DigiCert products, events, and promotions are also posted to our social media accounts so followers are the first to hear our exciting announcements.

twitter

Find us on Facebook

To find our official pages, simply click on the images above to start following DigiCert and become "in-the-know" for great information and announcements!

Upcoming Events

DigiCert will be exhibiting at several conferences this year, so come visit us if you're at the event!

Internet Retailer Conference & Exhibition 2011
June 14-17
San Diego, CA
Booth #1622

FOSE
July 19-21
Washington, DC
Booth #1707

Get a free exhibit hall only pass by using code DigiCertFOSE11 when registering on the FOSE website

2011 EDUCAUSE Annual Conference
October 18-21
Philadelphia, PA
Booth #113

Feedback? Article Suggestions? We want to know! Send an email to newsletter@digicert.com

DigiCert, Inc.
355 South 520 West
Canopy Building II
Lindon, UT 84042
+1-800-896-7973 ph
+1-866-842-0223 fax
www.digicert.com