



DigiCert Safe from Null Character Attacks

New attacks ineffective against DigiCert Certificates

During the recent Black Hat conference in Las Vegas, NV, Moxie Marlinspike demonstrated an attack against wildcard SSL certificates. This attack is carried out by inserting the "null" character (\0), which browsers recognize as a sign to stop checking the URL.

Once a certificate has been issued with the null character, the owner could theoretically use it on any domain. Since the browser would accept the certificate and not display a domain name mismatch error, users could easily be tricked into thinking the fraudulent site is legitimate.

DigiCert already had checks in place to ensure that this attack, or other attacks along this vector, are ineffective. A thorough audit confirms that no null character certificates have been issued by DigiCert. The ultimate resolution to this attack resides with an update to browser's software.

Marlinspike confirmed that this attack is

not possible against Extended Validation (EV) SSL certificates - yet another reason to put your trust in the highest level of authentication.

EV SSL Certificates enable special browser behavior (such as a green URL bar) to alert a site visitor that the site is encrypted and authenticated. Studies show that conversion rates for sites enabled with EV certificates are significantly higher than those without.

When building trust with your clients, remember that encryption is only half the battle. What is the value of encryption if you can't confirm who your data is being sent to? DigiCert's emphasis on strong authentication and powerful

encryption along with 24 hour dedicated support ensure you have the best

Call us toll free (Canada or US) at 1-800-896-7973 (international Customers please call us at +1-801-877-2100). Visit us online at www.digicert.com (24-hour Live Chat service provided).



- Recent DigiCert Clients**
- Environmental Protection Agency (EPA)
 - Social Security Administration (SSA)
 - Office Max
 - University of Southern California
 - Dartmouth College
 - Quicken Loans
 - City of Las Vegas
 - Opera Software ASA
 - Yamaha Corporation
 - Better Business Bureau
 - Trend Micro
 - U.S. Geological Survey
 - Fermi National Accelerator Laboratory
 - Wizards of the Coast, LLC
 - Archer Daniels Midland Company

Free DigiCert T-Shirt

As a special bonus for newsletter readers, DigiCert is giving away 100 free DigiCert T-Shirts. To receive your shirt, send an email to newsletter@digicert.com with the following information:

- Name
- Shipping address
- Account number (if applicable)
- How you heard about DigiCert
- Shirt size - S, M, L, XL, XXL
- Color - white, red, blue, or black

Enterprise Accounts Nearly Complete

M-PKI system simplifies certificate management

By: Travis Tidball, Director of Customer Relations

DigiCert is nearly prepared to launch its new enterprise-level Managed PKI service, which will allow organizations to have complete control over the management of their digital certificates, including real-time issuance, reissues and replacements, renewals, and revocations.

Organizations using the new M-PKI system will enjoy all the benefits offered with standard DigiCert services - top-notch support, strong encryption and compatibility, and terrific value - along with the ability to perform key life-cycle events on demand.

With Managed PKI, DigiCert will perform the validation of domains and

organizations ahead of time so that certificates can be issued immediately whenever they are needed. In this way, DigiCert maintains its high standards of validation, and clients are able to bypass the typical one-hour waiting period for their certificates.

Key features of DigiCert's Managed PKI include:

- Immediate Certificate Issuance
- Hierarchical account structure allows sub-accounts with limited permissions
- Approve or reject certificate requests while maintaining full management capabilities
- Reissue, Replace, and

Enterprise Account Access

Login to my account

Username:
(your email address in most cases)

Password:

[Forgot your password?](#)

revoke SSL certificates on demand

- Enable renewal notices for up to 60 days in advance of certificate expiration

If you would like to be notified when DigiCert's Managed PKI service launches, please go to <http://www.digicert.com/managed-pki-ssl.htm> or email mpki@digicert.com

5 Easy Steps for a Quick Certificate:

By: Flavio Martins, Director of Support & Validation

DigiCert can typically issue a certificate within two hours after an order has been received.

Here are some things you can do to ensure a certificate is issued as soon as possible:

1 - When ordering from within your account, select the correct company or create a new one if necessary.

2 - Be prepared to authorize the order via an email sent to the administrator of the domain.

3 - Double check to make sure the WHOIS record for your domain is current and publicly available.

4 - Make sure your organization is considered "Active" by the state / principality in which you are registered

5 - Update your legal registration and D&B records to show your most current address.

Be sure to give our Support & Validation staff a call at 1-800-896-7973 if you have any questions.

DigiCert Sponsors Online Trust Summit

Online Trust & Brand Protection Summit

by Ben Wilson, Legal Counsel



DigiCert is sponsoring the 2009 Online Trust & Brand Protection Summit, held on October 29th in Philadelphia, Pennsylvania. The program is described as:

"Full day intensive program designed to provide prescriptive guidance and advice to help protect your brand, enhance your reputation and build consumer trust. A must attend event for business and technical decision makers who are responsible

for creating and protecting brands including; privacy and public policy professionals, data stewards and interactive / email marketers."

Register by October 22nd and save \$100. <https://otalliance.org/events/Phila09.html>

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

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

All trademarks displayed on this publication are the exclusive property of the respective holders. To stop receiving publications, login to your DigiCert account, click on "Edit My Profile," and update your opt-in preferences.