Wednesday, November 14, 2018 at 4:18 PM

From: ICANN Global Support <noreply-globalsupport@icann.org>
Date: Wednesday, November 14, 2018 at 4:18 PM
Subject: TMDB Security Upgrades coming 10 December 2018

Dear ICANN Trademark Database User,

This is a reminder of upcoming changes to the security configuration of the Trademark Database.

As part of ICANN's commitment to security and stability, ICANN will be enhancing the security configuration on the Trademark Database (TMDB) interfaces. These changes will be effective in the production environment for the TMDB as of **10 December 2018**.

We strongly recommend that all users begin testing their systems as soon as possible.

To support users in preparing for these changes, ICANN initially deployed the TMDB Operational Testing & Evaluation (OT&E) systems for validation and testing beginning on **10 October 2018**. We have since learned that the 10 October 2018 deployment did not include full enforcement of the TLS 1.2 requirements. As of 7 November 2018, full enforcement of the TLS 1.2 requirement has been implemented in the OT&E system. If you tested your integration prior to 7 November, we suggest that you re-validate your systems.

The new settings for the OT&E systems are provided below:

The Transport Layer Security (TLS) implementation on the following (restricted access) URLs: https://ry.marksdb.org and https://tmcnis.org will be updated as follows:

- Only TLS v1.2 will be supported.
- Only the following ciphers will be permitted:
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
  - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
  - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

For any questions, please contact ICANN Global Support at: globalsupport@icann.org.

Best regards,

ICANN Global Support Center

_____

To reference past registry operator communications please click here.
To reference past registrar communications please click here.