Aktualizace protokolů

Níže naleznete seznam technologií, přes které mohou být vaše interní systémy napojeny. Zkontrolujte, prosím, své protokoly, zda jsou aktuální. Pokud nejsou, aktualizujte je na nejvyšší verzi.

Cílem je povolit pouze následující sady TLS1.2:

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-CHACHA20-POLY1305
- ECDHE-RSA-CHACHA20-POLY1305
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES256-GCM-SHA384

Curl:
Curl podporuje TLS1.2 počínaje 7.34.0. Pro zajištění kompatibility je potřeba curl aktualizovat na minimálně tuto verzi.

Aktuálně nainstalovanou verzi lze zjistit pomocí příkazu:

- curl --version

V závislosti na Linux distribuci lze aktualizaci provést pomocí správce balíčků, např:

- apt upgrade curl (APT)
- yum update curl (YUM)

Pro přesný postup, prosím, referujte dokumentaci využívané distribuce.

Java:
V Java 1.6, není TLS 1.2 podporované v Oracle public updates. Je podporovaná v Business Edition počínaje Oracle java version 6u115 b32.
V Java 1.7, je TLS1.2 podporované. Podporu lze zapnout přidáním startovacího parametru: -Dhttps.protocols="TLSv1.2″ -Djdk.tls.client.protocols="TLSv1.2″

Aktuálně nainstalovanou verzi Java je možné získat pomocí příkazu:

- java -version (jak na windows, tak na linux)

Aktualizovat verzi Java lze z ovládacího panelu Java:

- https://www.javatpoint.com/how-to-update-java
- Nebo stažením nejnovější verze: https://www.oracle.com/java/technologies/downloads/

Ruby:
Ruby používá systémovou knihiovnu OpenSSL, která podporuje TLS 1.2 by default od verze 1.0.1.

Aktuálně nainstalovanou verzi OpenSSL je možné získat pomocí příkazu:

- openssl version

Aktuální verze je k nalezení na:

- http://www.openssl.org/source/

Po stažení a extrahování balíčku je potřeba OpenSSL nainstalovat:

- # make clean
- # ./config shared –prefix=/usr –openssldir=/usr/local/openssl
- # make && make test
- # make install

Python:

Python používá systémovou knihiovnu OpenSSL, která podporuje TLS 1.2 by default od verze 1.0.1.

Aktuálně nainstalovanou verzi OpenSSL je možné získat pomocí příkazu:

- openssl version

Aktuální verze je k nalezení na:

- http://www.openssl.org/source/

Po stažení a extrahování balíčku je potřeba OpenSSL nainstalovat:

- # make clean
- # ./config shared –prefix=/usr –openssldir=/usr/local/openssl
- # make && make test
- # make install