

#####

Automatische Update Installation MSU Pakete - IngenServerHost @2019

#####

Ein Workaround für das TLS-Problem

Microsoft gibt im Supportbeitrag zwei Workaround an, mit dem sich das TLS-Timeout-Problem eventuell abschwächen lässt.

- Aktivieren Sie die Unterstützung für Extend Master Secret (EMS) Erweiterungen, wenn TLS-Verbindungen sowohl auf dem Client als auch auf dem Server-Betriebssystem durchgeführt werden. EMS gemäß [RFC 7627](#) wurde 2015 zu den unterstützten Versionen von Windows hinzugefügt. Jedes Update, das am oder nach dem 8. Oktober 2019 veröffentlicht wird, hat EMS standardmäßig für [CVE-2019-1318](#) aktiviert.
- Oder: Für Betriebssysteme, die kein EMS unterstützen, entfernen Sie die TLS_DHE_*-Cipher Suites aus der Liste der Chiffriersammlungen im Betriebssystem des TLS-Clients. Anweisungen dazu, wie Sie dies unter Windows tun, finden Sie unter [Prioritizing Schannel Cipher Suites](#).

Microsoft empfiehlt nicht, EMS zu deaktivieren. Wenn EMS explizit durch Administratoren deaktiviert wurde, kann es wieder aktiviert werden, indem man folgende Registrierungseinträge setzt. Im Schlüssel:

HKLM\System\CurrentControlSet\Control\SecurityProviders\Schannel

sind auf dem TLS-Server und -Client die folgenden Werte auf 0 zu setzen:

On TLS Server: *DisableServerExtendedMasterSecret*: 0

On TLS Client: *DisableClientExtendedMasterSecret*: 0

Damit sollten die TLS-Verbindungsprobleme weg sein.

Quelle: <https://www.borncity.com/blog/2019/10/30/windows-timeout-bei-tls-verbindungen-workaround/>

#####

Automatische Update Installation MSU Pakete - IngenServerHost @2019

#####

