T.C.
SOSYAL GÜVENLİK KURUMU BAŞKANLIĞI
Hizmet Sunumu Genel Müdürlüğü

20.03.2019

DUYURU

SOSYAL GÜVENLİK KURUMU SSL/TLS SERTİFİKASI TLS 1.2 KULLANIMI

Bilindiği gibi güvenliği düşük ağlarda kritik verilerin saldırganlardan korunması için SSL/TLS şifreleme teknikleri kullanılmaktadır. 1994 yılında ilk sürümü yayımlanmış olan SSL/TLS sistemi, zamanla artan güvenlik sağlayacak şekilde değişik sürümler yayımlamış, güvenliği düşük sürümler kullanımı zararlı olarak adlandırılarak kullanımdan yavaş yavaş kalkmıştır. Halihazırda SSL/TLS iletişimde, SSL 1.0, 2.0 ve 3.0 sürümleri modern sistemler tarafından güvenli kabul edilmeyerek kullanımı sonlanan, TLS 1.0 ve 1.1 sürümleri güvenilirliği nispeten daha yüksek ancak barındırdıkları güvenlik açıkları sebebiyle kullanılmaması gereken, TLS 1.2 sürümü ise güvenliği yüksek ve kullanılması gereken sürüm olarak yayımda bulunmaktadır.

07.12.2016 ve 13.01.2017 tarihli *"Sosyal Güvenlik Kurumu SSL/TLS Sertifikası TLS 1.2 Kullanımı"* konulu duyurular ile 03.01.2018 tarihi itibari ile *"SGK Kurum internet ve web servis uygulamalarına HTTPS erişiminde en az TLS 1.2 sürümü desteklenecektir."* bildirileri yapılmıştı.

Kurum uygulamalarına bağlanan bazı cihazların sürüm güncellemelerinin halen yapılamamasından dolayı TLS1.2 geçişi tamamlanmamış uygulamalar bulunmaktadır.

31.05.2019 tarihi itibari ile Kurum uygulamaları HTTPS bağlantılarında sadece TLS1.2 sürümünü desteklenecektir. Konu ile ilgili değişikliklerin bu tarihe kadar yapılması önem arz etmektedir.

Kurum internet uygulama kullanıcılarının uygulamalara daha güvenli bağlanabilmesi için kullandıkları cihazların işletim sistemi ve internet tarayıcılarını mümkün olan en son sürüm ve güncelleştirmeler ile kullanması Kurumumuz tarafından önerilmektedir.

Aşağıda Kurumumuz tarafından kullanımı önerilmeyen işletim sistemleri ve internet tarayıcıları sürümleri ile sadece tls1.2 ile erişim sunması hedeflenen(tls1.0 ve tls1.1 desteği kaldırılacak.) dns adresleri bulunmaktadır.

Bilgilerinizi rica ederim.

Birim Adı: SGK Hizmet Sunumu Genel Müdürlüğü

Kurumumuz Tarafından Kullanımı Önerilmeyen İşletim Sistemleri ve İnternet tarayıcıları:

- Kurum uygulamalarına tarayıcılar üzerinden bağlanan kullanıcıların en az Internet Explorer 11, Mozilla Firefox 45, Google Chrome 48 tarayıcı sürümlerini kullanması gerekmektedir.
- Kurum web servislerine bağlanan sunucuların en az Windows 2008 R2 sürümünde, Linux sürümleri için ise en az openssl 1.0.0.1e sürümünü kullanacak şekilde güncelleştirmeleri yapılmış olması gerekmektedir.
- Kullanılan web uygulama sunucuları için ise TLS1.2'yi varsayılan olarak destekleyen java8, netframework4.5 vb. uygulama yazılımlarının kullanılması önerilmektedir.
- Kurum uygulamalarına bağlanan istemcilerin işletim sistemi ve tarayıcı güncelleştirmelerinin yapılmış olması önemlidir. Microsoft Windows 7 sürümü altı işletim sistemleri, TLS 1.2 desteği sunmadığı için web servis ve internet explorer tarayıcısıyla erişimde problem yaşayacaktır. Google Chrome'un TLS 1.2 desteği Internet Explorer gibidir, Chrome da en az Windows 7 işletim sistemine gereksinim duymaktadır. Mozilla Firefox ise Windows 7 sürümü altı işletim sistemlerinde(en az Windows XP sp2), TLS 1.2 desteği vermektedir. Belirtilen tarih sonrası Windows 7 altı sistemlerden Kurum uygulamalarımıza bağlanmak isteyenler yukarıda en azı belirtilen Firefox sürümü ile uygulamalarımıza bağlantı kurabilecekleridir.

Sadece TLS1.2 ile erişim sunması hedeflenen(tls1.0 ve tls1.1 desteği kaldırılacak) dns adresleri:

- net.sgk.gov.tr
- netws.sgk.gov.tr
- hitap.sgk.gov.tr
- ebildirge.sgk.gov.tr
- uyg.sgk.gov.tr
- wsbanka.sgk.gov.tr
- kesenek.sgk.gov.tr
- testkamu.sgk.gov.tr
- uygkamu.sgk.gov.tr
- ehaciz.sgk.gov.tr
- kadim.sgk.gov.tr
- kesenek.sgk.gov.tr
- huyap.sgk.gov.tr