Insecure Transportation Security Protocol Supported (SSLv2 and SSLv3)

a. SSL / TLS Nedir?

SSL Netscape şirketi tarafından 1994 yılında World Wide Web'de güvenli iletişim kurma amacıyla geliştirilmiştir. Ardından Internet Engineering Tast Force kuruluşu aynı işlevi gerçekleştiren standard bir protokol geliştirme işine girişmiştir. Bu iş için SSL 3.0 'ı temel almışlardır ve 1999 yılında SSL'in yeni bir versiyonu olan TLS protocol'ünü geliştirmişlerdir.

SSL ve TLS web tarayıcı ve sunucu arasındaki iletişimde güvenli trafiği temin eden en yaygın protokoller olarak bilinirler. SSL ve TLS aynı zamanda başka uygulama katmanı protokollerce de kullanılabilmektedir. Örneğin File Transfer Protocol (FTP), Lightweight Directory Access Protocol(LDAP) ve Simple Mail Transfer Protocol (SMTP) gibi. SSL ve TLS sunucu yetkilendirmesini, istemci yetkilendirmesini, veri şifrelemesini ve veri bütünlüğünü World Wide Web gibi network'lerde sağlamaktadır.

b. Insecure Transportation Security Protocol Supported (SSLv2 and SSLv3) Zafiyeti Nedir?

IETF kuruluşu hem SSL 2.0 yi hem de 3.0 ü (yani SSLv2 ve SSLv3 ü) 2011 ve 2015 yıllarında artık eski protokol olarak kabul edip rafa kaldırmıştır. Çünkü yıllar içerisinde çeşitli zafiyetlere sahip oldukları (örn; DROWN ve POODLE gibi) görülmüştür. Çoğu modern tarayıcı eğer web sunucusu SSLv2 ya da SSLv3'ü kullanıyorsa URL çubuğunda güvenlik uyarısı vermektedir. Bu nedenle web geliştiricileri olarak web sunucularında SSLv2 ve SSLv3 yapılandırmalarını disable etmeli, TLS protokolünü enable etmeliyiz.

c. SSLv3 mi TLS mi kullanılmalı?

SSLv3 mi yoksa TLS mi kullanılmalı sorusunun cevabı kesinlikle TLS kullanılmalıdır. bkz. https://luxsci.com/blog/ssl-versus-tls-whats-the-difference.html

d. Insecure Transportation Security Protocol Supported (SSLv2 and SSLv3) Zafiyeti Nasıl Kapatılır?

Uyarı

> Netsparker : Insecure Transportation Security Protocol Supported (SSLv2) [Critical]
> Netsparker : Insecure Transportation Security Protocol Supported (SSLv3) [Medium]

Web sunucusunda SSLv2 ve SSLv3 protokollerini disable etmek ve TLS'i enable etmek için aşağıdaki yapılandırma ayarları yapılmalıdır.

> Not: Apache de ssl disable etme ve tls enable yi uygulamalı olarak görmek için bkz. Ubuntu Masaüstü / Paketleme için Gözden Geçirilecekler / Sıkılaştırmalar / Apache Sunucuda SSL Disable Etme ve TLS Enable Etme.docx

```
# Apache sunucular için
sudo a2enmod ssl                                  // apache şifreleme modülü enable olur.
sudo nano /etc/apache2/apache2.conf               // apache yapılandırma dosyası açılır.
# apache2.conf dosyasının en altına aşağıdaki girilir.
SSLProtocol -all +TLSv1.1 +TLSv1.2
```

IIS sunucular için
- Başlat > Çalıştır > regedit
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ SecurityProviders\ SCHANNEL\Protocols\SSL 2.0\ konumuna git.
- Eğer Client isimli klasör yoksa SSL 2.0 klasörüne sağ tıkla, New -> Key yap ve Client isimli konum oluştur.
- Client isimli konuma sağ tıkla ve New -> DWORD yap. Gelen ekrandaki value name kısmına DisabledByDefault isimini, value data kısmına ise 1 rakamını ekranda yer alan hex radio button'u seçili iken gir.
- SSL 2.0 klasöründe eğer Server isimli klasör yoksa SSL 2.0 klasörüne sağ tıkla, New -> Key yap ve Server isimli konum oluştur.
- Server isimli konuma sağ tıkla ve New -> DWORD yap. Gelen ekrandaki value name kısmına Enabled ismini, value data kısmına ise 0 rakamını ekranda yer alan hex radio button'u seçili iken gir. Ardından IIS sunucuyu
yeniden başlat.

Böylece IIS sunucuda SSLv2 disable olur. SSLv3 için aynı adımlar Protocols altındaki SSL 3.0 klasöründe takip edilir (yoksa oluşturulur ve aynı adımlar takip edilir). IIS sunucuda TLS 'i enable etmek için ise

- Başlat > Çalıştır > regedit
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ SecurityProviders\SCHANNEL\Protocols konumuna git.
- Protocols klasörüne sağ tık yapıp New -> Key diyerek TLS 1.2 isimli konum oluştur.
- TLS 1.2 klasörüne sağ tık yapıp New -> Key diyerek Client isimli konum oluştur.
- Client klasörüne sağ tık yapıp New -> DWORD de. Gelen ekrandaki value name kısmına Enabled isimini, value data kısmına ise 1 rakamını ekrandaki hex radio button'u seçili iken gir.
- Client klasörüne sağ tık yapıp New -> DWORD de. Gelen ekrandaki value name kısmına DisabledByDefault, value data kısmına ise 0 rakamını ekranda yer alan hex radio button'u seçili iken gir.
- TLS 1.2 klasörüne sağ tık yapıp New -> Key diyerek Server isimli konum oluştur.
- Server klasörüne sağ tık yapıp New -> DWORD de. Gelen ekrandaki value name kısmına Enabled, value data kısmına ise 1 rakamını ekranda yer alan hex radio button'u seçili iken gir.
- Server klasörüne sağ tık yapıp New -> DWORD de. Gelen ekrandaki value name kısmına DisabledByDefault, value data kısmına ise 0 rakamını ekranda yer alan hex radio button'u seçili iken gir. Ardından IIS sunucuyu yeniden başlat.

Not: Easyfix adlı tool yukarıda anlatılan adımları otomatikmen yapıyormuş. Ancak ingilizce dışında bir dil paketi windows 'da yüklü ise sorun çıkarıyormuş. O nedenle kullanımı gösterilmemiştir.

adımları uygulanır. Böylece apache ve IIS web sunucularında SSL'ler disable, TLS ise enable edilmiş olur.

Kaynaklar

https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/insecure-transportation-security-protocol-supported-sslv2/

https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/insecure-transportation-security-protocol-supported-sslv3/

http://www.wikizero.info/index.php?q=aHR0cHM6Ly9lbi53aWtpcGVkaWEub3JnL3dpa2kvUE9PRExF

https://technet.microsoft.com/en-us/library/cc784450(v=ws.10).aspx

https://www.globalsign.com/en/blog/ssl-vs-tls-difference/

https://www.digicert.com/ssl-support/iis-disabling-ssl-v3.htm

https://support.quovadisglobal.com/kb/a433/how-to-enable-tls-1_2-on-windows-server-2008-r2.aspx

https://support.microsoft.com/en-us/help/3140245/update-to-enable-tls-1-1-and-tls-1-2-as-a-default-secure-protocols-in

https://luxsci.com/blog/ssl-versus-tls-whats-the-difference.html