# Bilgi Sistemleri ve Güvenliği

**170542018**

**Mustafa Ali Kağan Küçük**

## Weak Ciphers Enabled (Zayıf Şifreler Etkin)



**MEDIUM**

### Özet

Invicti, güvenli iletişim (SSL) sırasında zayıf şifrelerin etkinleştirildiğini tespit etti.

Ziyaretçilerinizle güvenli iletişimi korumak için web sunucunuzda yalnızca güçlü şifrelere izin vermelisiniz.

### Etki

Saldırganlar, sunucunuz ve ziyaretçileriniz arasındaki SSL trafiğinin şifresini çözebilir.

### Yapılacak İşlemler

1. Apache için, httpd.conf içindeki SSLCipherSuite yönergesini değiştirmelisiniz.

SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4

1. Lighthttpd yazılımına bu kısımları eklemeliyiz:

ssl.honor-cipher-order = "enable" ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"

1. Microsoft IIS için sistem kayıt defterinde bazı değişiklikler yapmalısınız. **Kayıt defterini yanlış düzenlemek, sisteminize ciddi şekilde zarar verebilir. Kayıt defterinde değişiklik yapmadan önce, bilgisayarınızdaki tüm değerli verileri yedeklemelisiniz.**
   1. Başlat'a tıklayın, Çalıştır'a tıklayın, yazın regedt32veya yazın regeditve ardından Tamam'a tıklayın.
   2. Kayıt Defteri Düzenleyicisi'nde aşağıdaki kayıt defteri anahtarını bulun: HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders
   3. Aşağıdaki kayıt defteri anahtarları için "Etkin" DWORD'yi "0x0" olarak ayarlayın:

SCHANNEL\Ciphers\DES 56/56 SCHANNEL\Ciphers\RC4 64/128 SCHANNEL\Ciphers\RC4 40/128 SCHANNEL\Ciphers\RC2 56/128 SCHANNEL\Ciphers\RC2 40/128 SCHANNEL\Ciphers\NULL SCHANNEL\Hashes\MD5

YÜKSEK - Triple-DES kullanan tüm şifreler etkinleştirilir ORTA - 128 bit şifrelemeli tüm şifreler etkinleştirilir

!aNULL - Boş kimlik doğrulama devre dışı bırakılır ve daha sonra bir "+" (artı) işareti aracılığıyla dizeye yeniden eklenemez

!MD5 - MD5 karma devre dışı bırakılır ve daha sonra "+" (artı) işaretiyle dizeye yeniden eklenemez.

$ openssl ciphers 'HIGH' ADH-AES256-SHA:DHE-RSA-AES256-SHA:DHE-DSS-AES256-SHA:AES256- SHA:ADH-AES128-SHA:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA:

AES128-SHA:ADH-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:EDH-DSS-DES-CBC3-SHA:DES-CBC3- SHA:DES-CBC3-MD5

$ openssl ciphers 'MEDIUM' ADH-SEED-SHA:DHE-RSA-SEED-SHA:DHE-DSS-SEED-SHA:SEED-SHA:ADH- RC4-MD5:RC4-SHA:RC4-MD5:RC2-CBC-MD5:RC4-MD5

$ openssl ciphers 'LOW' ADH-DES-CBC-SHA:EDH-RSA-DES-CBC-SHA:EDH-DSS-DES-CBC-SHA:DES-

CBC-SHA:DES-CBC-MD5

tüm SSLCipherSuite dizesini 'openssl şifreleri' ile de belirtebilirsiniz.

"güçlü" tanımı, istediğiniz kullanım durumlarına, tehdit modellerinize ve kabul edilebilir risk seviyelerinize bağlıdır. Apache HTTP Sunucusu ekibi bunları sizin için belirleyemez. *Güçlü şifrelemenin* tek başına

güçlü *güvenlik* sağlamadığını lütfen unutmayın.

Lighttpd(lighty), hızlı, güvenli, esnek ve standartlara sadık olacak şekilde tasarlanmış bir web sunucusudur. Hızın çok önemli olduğu ortamlar için optimize edilmiştir. Bunun nedeni, diğer sunuculardan daha az CPU ve RAM tüketmesidir.

Lighttpd, yük sorunları olan herhangi bir sunucu için uygundur. Ücretsiz bir yazılımdır ve BSD lisansı altında dağıtılmaktadır. Resmi olarak GNU / Linux ve UNIX üzerinde çalışır.

Microsoft Windows için Kevin Worthington tarafından sağlanan Lighttpd For Windows olarak bilinen bir dağıtım vardır.

### Düzeltme

Web sunucunuzu zayıf şifrelerin kullanılmasına izin vermeyecek şekilde yapılandırın.

## ViewState is not Encrypted ViewState Şifreli değil



**LOW**

### Özet

Invicti, ViewState Şifrelemenin devre dışı bırakıldığını tespit etti. ASP.NET görünüm durumu, geri göndermeler arasında bir Web Formunun durumundaki değişiklikleri sürdürmek için bir ASP.NET Web sayfası tarafından kullanılan tekniktir. Varsayılan olarak, görünüm durumu verileri sayfada gizli bir alanda depolanır ve base64 kodlaması kullanılarak kodlanır.

Görüntüleme durumu verileri şifrelenmez, bu nedenle hala görüntülenebilir ve potansiyel olarak kötü niyetli kullanıcılar tarafından ele geçirilip okunabilir. Ancak bazı durumlarda kontroller, hiçbir kullanıcının erişmemesi gereken bilgileri depolamak için görünüm durumunu kullanabilir. Örneğin, sayfa, öğe tanımlayıcılarını (veri anahtarlarını) görünüm durumunda saklayan bir veriye bağlı denetim içerebilir.

### Etki

Saldırgan, olası güvenlik açıkları için uygulamanın durum yönetimi mantığını inceleyebilir; uygulamanız, uygulama açısından kritik bilgileri ViewState'te saklarsa, bu bilgiler de ortaya çıkar.

### Düzeltme

ASP.NET, ViewState parametreleri için şifreleme sağlar.

Sayfa tabanlı koruma için, aşağıdaki yönergeyi etkilenen sayfanın en üstüne yerleştirin.

<%@Page ViewStateEncryptionMode="Always" %>

web.configBu seçeneği, dosyaları kullanarak tüm uygulama için de ayarlayabilirsiniz

. web.configUygulamanızın dosyası için aşağıdaki yapılandırmayı uygulayın .

<System.Web>

<pages viewStateEncryptionMode="Always">

</System.Web>