Version Disclosure(ASP.NET)

**Özet**

Invicti, hedef web sunucusunun HTTP yanıtında bir sürüm ifşası (ASP.NET) belirledi.

Bu bilgiler, bir saldırganın kullanılan sistemleri daha iyi anlamasına ve potansiyel olarak ASP.NET'in belirli sürümünü hedefleyen başka saldırılar geliştirmesine yardımcı olabilir.

**Etki**

Saldırgan, açıklanan bilgileri, tanımlanan sürüm için belirli güvenlik açıklarını toplamak için kullanabilir.

**Düzeltme**

Özel hata sayfaları kullanarak ve HTTP yanıtlarından web.configkaldırarak bilgi sızıntısını önlemek için aşağıdaki değişiklikleri dosyanıza uygulayın .X-AspNet-Version

<Sistem.Web>

<httpRuntime enableVersionHeader="false" />

<customErrors mode="Açık" defaultRedirect="~/error/GeneralError.aspx">

<error statusCode="403" yönlendirme="~/error/Forbidden.aspx" />

<error statusCode="404" yönlendirme="~/error/PageNotFound.aspx" />

<error statusCode="500" yönlendirme="~/error/InternalError.aspx" />

</customErrors>

</Sistem.Web>

Insecure Transportation Security Protocol Supported (TLS 1.0)

**Özet**

Invicti, güvenli olmayan ulaşım güvenlik protokolünün (TLS 1.0) web sunucunuz tarafından desteklendiğini tespit etti.

TLS 1.0'ın birkaç kusuru vardır. Saldırgan bağlantı hatalarına neden olabilir ve BEAST (SSL/TLS'ye Karşı Tarayıcı İstismarı) gibi güvenlik açıklarından yararlanmak için TLS 1.0 kullanımını tetikleyebilir.

TLS 1.0 kullanan web siteleri, 30 Haziran 2018'den beri PCI tarafından uyumlu değildir.

**Etki**

Saldırganlar, ortadaki adam saldırıları gerçekleştirebilir ve web siteniz ile ziyaretçileri arasındaki şifreleme trafiğini gözlemleyebilir.

**Yapılacak İşlemler**

TLS 1.0'ı devre dışı bırakmanızı ve bunu TLS 1.2 veya üstü ile değiştirmenizi öneririz. Daha fazla ayrıntı için Çözüm bölümüne bakın.

**Düzeltme**

Web sunucunuzu zayıf şifrelerin kullanılmasına izin vermeyecek şekilde yapılandırın. Değişiklikleri etkinleştirmek için web sunucusunu yeniden başlatmanız gerekir.

Apache için mod\_ssl modülü tarafından sağlanan SSLProtocol yönergesini ayarlayın. Bu yönerge, sunucu düzeyinde veya sanal ana bilgisayar yapılandırmasında ayarlanabilir.

SSLProtokol +TLSv1.2

nginx.confNginx için, dosyada ssl\_protocols yönergesinin herhangi bir kullanımını bulun ve TLSv1.

ssl\_protocols TLSv1.2;

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.

Başlat'a ve ardından Çalıştır'a tıklayın, regedt32veya yazın regeditve ardından Tamam'a tıklayın.

Kayıt Defteri Düzenleyicisi'nde aşağıdaki kayıt defteri anahtarını bulun veya yoksa oluşturun:

HKEY\_LOCAL\_MACHINESYSTEMCurrentControlSetControlSecurityProvidersSCHANNELProtokollerTLS 1.0

Adlandırılmış bir anahtar bulun Serverveya yoksa oluşturun.

Anahtarın altında, mevcut değilse veya oluştur Serveradlı bir DWORD değeri bulun ve değerini "0" olarak ayarlayın.Enabled

Lighttpd için yapılandırma dosyanıza aşağıdaki satırları koyun:

ssl.use-sslv2 = "devre dışı bırak"

ssl.use-sslv3 = "devre dışı bırak"

ssl.openssl.ssl-conf-cmd = ("Protokol" => "-TLSv1.1, -TLSv1, -SSLv3") # v1.4.48 veya üzeri

ssl.ec-eğrisi = "secp384r1"